UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Potential Enhancements to the Critical Infrastructure Protection Reliability Standards	)	Docket No. RM20-12-000

COMMENTS OF THE EDISON ELECTRIC INSTITUTE AND THE ELECTRIC POWER SUPPLY ASSOCIATION

The Edison Electric Institute ("EEI") and the Electric Power Supply Association ("EPSA") submit these comments in response to the Notice of Inquiry ("NOI") issued by the Federal Energy Regulatory Commission ("Commission") on June 18, 2020, in the above-captioned docket. The Commission seeks comments on certain potential enhancements to the currently-effective Critical Infrastructure Protection ("CIP") Reliability Standards, specifically whether the CIP Reliability Standards adequately address low impact BES Cyber Systems[1] with respect to three topics: (i) cybersecurity risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events that are derived from the National Institute of Standards and Technology ("NIST") "Framework for Improving Critical Infrastructure Cybersecurity" ("NIST Framework").[2] In addition, the Commission seeks

[1] "BES Cyber System" is a NERC-defined, Commission-approved definition that means "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." A BES Cyber Asset is a "Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." A Cyber Asset is a "programmable electronic devices, including the hardware, software, and data in those devices." See NERC Glossary of Terms, Updated June 2, 2030. https://www.nerc.com/files/glossary_of_terms.pdf.

[2] "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, National Institute of Standards and Technology April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether Commission action, including potential modifications to the CIP Reliability Standards, would be appropriate to address such risk.[3]

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for over 220 million Americans and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. EEI's members are committed to providing affordable and reliable electricity to customers now and in the future. EEI's members include generator owners and operators, transmission owners and operators and other entities that are subject to the mandatory CIP Reliability Standards.

EPSA is the national trade association representing leading independent power producers and marketers. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. EPSA seeks to bring the benefits of competition to all power customers. EPSA member companies are generation owners and operators that are subject to the mandatory CIP Reliability Standards in that capacity. The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

As further explained below, the issues raised in the NOI are covered under existing and/or soon to be implemented CIP Reliability Standards. These changes will require utilities to enhance their existing security for certain aspects of the Bulk-Power System ("BPS"). The Commission should reconsider any additional enhancements until after these standards have

---

[3] *Potential Enhancements to the Critical Infrastructure Protection Reliability Standards,*171 FERC ¶ 61,215 (2020)("NOI").

been in place for a period of time. Experience with these standards will better inform any potential future Commission action in this area. This also would be consistent with NERC's risk-based focus and the Commission's flexible approach to Reliability Standards.

I. BACKGROUND

Protecting the nation's energy infrastructure from cybersecurity threats is a top priority for the nation's electric companies. Electric companies manage and mitigate risk by taking a risk-based "defense-in-depth" approach to protecting critical energy grid assets from threats. This approach encompasses compliance with the Reliability Standards in addition to activities that surpass the mandatory requirements.

NERC is charged with developing and enforcing Reliability Standards that provide for an "adequate level of reliability" of the BPS pursuant to its mission of assuring the effective and efficient reduction of risks to the reliability and security of the BPS and takes a risk-based focus to mitigate risks. The Commission supports NERC's risk-based approach that is directed towards activities with a greater potential impact on reliability.

The Standards provide a foundation for strengthening the industry's cybersecurity posture. The CIP Reliability Standards employ a risk-based approach that provides for an efficient and effective allocation of resources protecting critical infrastructure, providing regulatory certainty and maximizing overall benefits to reliability while allowing registered entities to focus properly on those elements that pose the most risk to reliability and include certain requirements for low impact systems. For example, Reliability Standard CIP-002-5.1a requires entities to identify BES Cyber Systems and categorize them as low, medium, or high-impact systems based upon the adverse impact that loss, compromise, or misuse of those systems could have on bulk power system reliability.

On the other hand, the NIST Framework consists of voluntary guidelines and practices to promote the protection of critical infrastructure. The NIST Framework consists of five functions that each provide a high-level, strategic view of one part of an organization's cybersecurity risk management. Each of the five functions is composed of categories and subcategories, with the five functions having a total of 23 categories and 108 subcategories. Categories are defined as cybersecurity outcomes closely tied to programmatic needs and activities.

II. COMMENTS

In the NOI, the Commission explains that Commission staff reviewed the NIST Framework, compared it with the substance of the CIP Reliability Standards and identified certain topics addressed in the NIST Framework that it believes may not be adequately addressed in the CIP Reliability Standards. In particular, the Commission contends that three subcategories of the NIST Framework—(i) risks pertaining to data security, (ii) detection of anomalies and events, and (iii) mitigation of cybersecurity events—have no corresponding requirement for low impact BES Cyber Systems.

The NIST Framework's scope, model, and focus are different from NERC Reliability Standards. Nevertheless, in developing the current "Version 5" of the CIP Reliability Standards, NERC drew, in part, from the NIST concepts. Additionally, a recent mapping of the CIP Reliability Standards to the NIST Framework conducted by NERC and NIST revealed a great deal of alignment between the two.[4]

The NOI expresses concern that some of the CIP Reliability Standards do not apply to low impact BES Cyber Systems. The Electric Reliability Organization ("ERO"), with oversight

[4] The mapping document can be found on NERC's website, https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx.

by the Commission, is charged with developing and enforcing Reliability Standards that provide for an "adequate level of reliability" of the BPS. NERC, as the ERO certified pursuant to section 215(c) of the Federal Power Act, pursues its mission of assuring the effective and efficient reduction of risks to the reliability and security of the BPS. NERC's strategic plan emphasizes a risk-based focus, noting that "[a]s reliability and security risks emerge quickly, coordinated and swift development of improved processes, tools, and simulation models provide a strong foundation and catalyst to mitigate these risks."[5] For years, the Commission has acknowledged and approved NERC's risk-based approach that directs efforts towards activities with a greater potential impact on bulk electric system reliability.[6] It is important to achieve reliability risk mitigation, and NERC's overall approach to risk is consistent with this pursuit.

This risk-based approach is reflected in the CIP Reliability Standards. For example, Reliability Standard CIP-003-8, which became effective earlier this year, includes policies for assets containing low impact systems. Requirement R2 requires entities to develop and implement cybersecurity plans to meet specific security control objectives for assets containing low impact BES Cyber Systems. The cybersecurity plan covers five subject matter areas: (1) cybersecurity awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) transient cyber asset and removable media malicious code risk mitigation. The plan, along with the cybersecurity policies required under Requirement R1 Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems. Each responsible entity with at least one asset identified in Reliability Standard CIP-002 containing low impact BES Cyber Systems must implement a

[5] *ERO Enterprise Long-Term Strategy* (Dec. 12, 2019) at 2.

[6] *See Order on Electric Reliability Organization Risk Based Registration Initiative and Requiring Compliance Filing*, 150 FERC ¶ 61,213 (2015).

cybersecurity plan for its low impact BES Cyber Systems, which is consistent with NERC's and the Commission's endorsement of a risk-based approach.

Nevertheless, NERC and industry are aware of the need to evaluate threats, vulnerabilities and resulting risks to determine appropriate tools for addressing the risks such as modifications to the standards. As an example, Project 2020-03 is a NERC board-endorsed project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary. To the extent not already covered by the CIP Reliability Standards, this project will encompass the Commission's concern in the NOI regarding the NIST controls for detection of anomalies and further mitigates the potential risk of a coordinated cyberattack on geographically distributed low impact BES Cyber Systems.

In addition, several new CIP Reliability Standards will be subject to enforcement soon, and others have been modified and will also be coming into effect in the near term.[7] Before the Commission takes any action on this NOI, it should allow stakeholders to gain experience from implementation of these standards, which will better inform issues raised in the NOI. Such action would be consistent with NERC's risk-based focus and the Commission's flexible approach to Reliability Standards.[8]

[7] *See, e.g.*, Reliability Standards CIP-013 (Supply Chain Risk Management), and CIP-010-3 (Configuration Change Management and Vulnerability Assessments) become effective October 1, 2020, and Reliability Standard CIP-012-1 (Communications between Control Centers) becomes effective October 1, 2022.

[8] *Revised Critical Infrastructure Protection Reliability Standards*, 156 FERC ¶ 61,050 (2016).

A. Comments on NIST Framework Issues

The Commission is exploring whether the CIP Reliability Standard requirements corresponding to three subcategories in the NIST Framework (data security, anomalies and events, and mitigation) could represent a potential gap in the CIP Reliability Standards.

1. Data Security Category

The NIST Framework data security category specifies activities to manage information and records consistent with an organization's risk strategy to protect the confidentiality, integrity, and availability of information and data. The Commission staff analysis indicates that two NIST data security subcategories may not be adequately addressed in the CIP Reliability Standards. Under the subcategory "adequate capacity to ensure availability is maintained," Reliability Standard CIP-011-2 and Reliability Standard CIP-012-1 address real-time assessment and real-time monitoring data while being transmitted between any applicable control center. For the subcategory pertaining to integrity checking mechanisms to verify software, firmware, and information integrity, the NOI contends that there is partial coverage by Reliability Standard CIP-013-1.

EEI and EPSA Comments

The CIP Reliability Standards provide support for protecting cyber assets against compromises that could lead to misoperation or instability in the BES, such as digital relays that control transmission breakers.[9] Since their inception, the CIP Reliability Standards have focused on protecting cyber assets with data-at-rest protection included as part of the cyber asset protection. NERC defines a Cyber Asset as "[p]rogrammable electronic devices, including the

[9] *See, e.g.,* Reliability Standards CIP-002, 3 and 5

hardware, software, and data in those devices."[10] For data in motion, Reliability Standard CIP-012-1, which will become effective on July 1, 2022, is intended to protect the confidentiality and integrity of real-time assessment and monitoring data transmitted between control centers, which protects the confidentiality and integrity of data flowing between control centers of all impact categories: high, medium, and low.

In addition, BES Cyber System Information – the sensitive system data that could potentially be used maliciously to disrupt operations – is covered by Reliability Standard CIP-011. Requirement R1, Part 1.2 requires responsible entities to protect and secure BES Cyber System Information, including storage, transit, and use. It also requires protections against data leaks. Requirement R2, Part 2.1 states that prior to the release for reuse of applicable cyber assets that contain BES Cyber System Information, the responsible entity must act to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. Data is also protected by removal, transfers, and disposition as required by Requirement R2.2, which states that prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the responsible entity must act to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

Other CIP Reliability Standards also address information management pertaining to confidentiality, integrity and availability regarding capacity to ensure availability. Reliability Standard CIP-009-6 Requirement R1 requires registered entities to specify recovery plan requirements in support of the continued stability, operability, and reliability of the BES and to have documented recovery plans for the backup and storage of information required to recover BES Cyber System functionality. Reliability Standard CIP-010 is intended to aid registered

[10] *See* NERC Glossary of Terms, https://www.nerc.com/files/glossary_of_terms.pdf.

entities in preventing and detecting unauthorized changes to certain critical cyber assets by specifying configuration change management and vulnerability assessment requirements in support of protecting the assets from compromise that could lead to mis-operation or instability.

2. Anomalies and Events Category

In the NOI, the Commission describes a potential gap between the NIST Framework "anomalies and events" category and the Reliability Standard CIP-008-5 incident response requirements because applicable entities have a process to "identify, classify, and respond to Cyber Security Incidents," for medium and high impact BES Cyber Systems but there is no requirement for low impact BES Cyber Systems.

EEI and EPSA Comments

The CIP Reliability Standards currently address detection and mitigation of anomalous activity for BES Cyber Systems in control centers, such as Reliability Standard CIP-005-5 Requirement R1 that requires entities to have methods for detecting known or suspected malicious communications for both inbound and outbound communications. Reliability Standard CIP-007-6 Requirement R4 mandates implementation of a process that collectively includes logging events for identification, and after-the-fact investigations, of cybersecurity incidents that include the detection of failed login attempts, successful logins, and malicious code. Reliability Standard CIP-003-8 requires responsible entities with at least one asset identified in CIP-002 containing low impact BES Cyber Systems to implement cyber security plans for its low impact BES Cyber Systems, permitting only necessary inbound and outbound electronic access, such that denied outbound traffic can be used to detect anomalous events or compromise.

Furthermore, the NERC Project 2020-03 modifying Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems will further enhance the detection of known or suspected anomalous communications, both inbound and outbound, as well as the initiation of active vendor remote access sessions, and would therefore include the disabling of anomalous remote access when necessary.

3. Mitigation Category

In the NOI, the Commission explains that the NIST Framework mitigation category specifies activities to prevent the expansion of a cybersecurity event, mitigate any effects and resolve the incident. The NIST Framework also identifies internal controls in three subcategories requiring that incidents are contained and mitigated and that newly identified vulnerabilities are mitigated or documented as accepted risks. The Commission cites Reliability Standard CIP-008-5 as requiring responsible entities to document their cybersecurity incident response plans and provide evidence of incident response processes or procedures that address incident handling, but notes that it does not specifically require incident containment or mitigation as discussed in the three mitigation subcategories and that it does not apply to low impact BES Cyber Systems. The Commission also points to Reliability Standard CIP-010-2 as addressing the need to mitigate newly identified vulnerabilities for medium and high impact BES Cyber Systems, but not for low impact BES Cyber Systems.

EEI and EPSA Comments

The CIP Reliability Standards adequately address the mitigation subcategories, and registered entities have controls to identify and prioritize assets based on their risk to the interconnected transmission network. The purpose of Reliability Standard CIP-008 is to mitigate, by specifying incident response requirements, the risk to the reliable operation of the

BES or a BES Cyber System (a Cyber Security Incident) as the result of compromises, or attempts to compromise, or disrupt electronic or physical security perimeters. Reliability Standard CIP-008-5 Requirement R1, Part 1.1 requires one or more processes to identify, classify, and respond to Cyber Security Incidents. Reliability Standard CIP-008-5 Requirement R1, Part 1.4 concerns incident handling procedures for Cyber Security Incidents and explains that registered entities can use dated Cyber Security Incident response processes or procedures that address incident handling which includes containment (i.e., mitigation), eradication, and recovery/incident resolution. Requirement R2, Part 2.2 requires responsible entities to implement the plan, including incident handling procedures, when responding to a Reportable Cyber Security Incident. The implementation of a Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to responsible entities for improving security controls.

Reliability Standard CIP-003-8 Requirement R2 requires responsible entities who have assets identified in CIP-002 as containing low impact BES Cyber Systems to implement one or more cyber security plan(s) for its low impact BES Cyber Systems. Attachment 1 contains additional requirements for cybersecurity plans for those assets containing low impact BES Cyber Systems. Section 4.4 of Attachment 1 requires responsible entities to include incident handling of a Cyber Security Incident as part of their cyber security plans for assets containing low impact BES Cyber Systems. These requirements address the mitigation of cyber security incidents for all assets containing low impact BES Cyber Systems.

B. Coordinated Cyberattack Assessment

The NOI seeks comment on the risk of a coordinated cyberattack on the BES and the potential need for Commission action to address such risk, claiming an increasing number of

generation resources are categorized as low impact BES Cyber Systems and therefore are not required to comply with the full suite of CIP Reliability Standards. The Commission seeks comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether modifications to the CIP Reliability Standards, including potential modifications to the current megawatt thresholds, would be appropriate to address such risks. In particular, the Commission seeks comment regarding the procedures and security controls that are currently employed to protect against the potential risk of a geographically distributed coordinated cyberattack and whether modifications to the CIP Reliability Standards would be appropriate to address such risks.

EEI and EPSA Comments

Protecting the nation's energy grid and ensuring a reliable, resilient, and affordable supply of energy are top priorities for electric companies. EEI and EPSA members' risk-based approach encompasses compliance with Reliability Standards and activities that go beyond those baseline requirements. EEI and EPSA members use numerous procedures, security controls, tools, tactics, and strategies, as well as engage in a variety of programs and partnerships to protect and support grid reliability. This includes deploying many tools and technologies that improve situational awareness and communication of actionable intelligence and threat indicators in a timely manner to appropriate industry and government personnel; preparing for and exercising emergency response procedures to both natural and manmade threats to energy grid operations; and working closely with other interdependent critical infrastructure sectors to enhance collective preparation and response to threats against the grid.

Reliability Standard CIP-003 is one of the many tools that industry uses to address the risk of a coordinated attack on the grid, as it addresses key areas important to mitigating a

coordinated cyberattack: electronic access controls on external connectivity, incident response plans, and transient cyber assets and removable media. For each asset containing low impact BES Cyber System identified pursuant to Reliability Standard CIP-002, the responsible entity is required to implement electronic access controls on external connectivity. This Standard helps protect against coordinated cyberattacks by focusing on protecting the external connectivity, that is, the networks that allow assets containing low impact BES Cyber Systems to communicate with each other. It is these networks that are a potential vector for coordinated cyberattack. This requirement limits external connectivity to only what is necessary for operation, for both inbound and outbound data. This reduces the available attack surface of all low impact BES Cyber Systems in the entire BES. It also reduces the risk of any low impact system communicating to unknown systems, such as attacker command and control hosts used to initiate a coordinated cyberattack.

In addition, Reliability Standard CIP-003-8 requires all assets containing low impact BES Cyber Systems to have documented and tested incident response plans for cybersecurity incidents. All assets containing low impact BES Cyber Systems also are required to have methods to mitigate the propagation of malware from temporary portable devices and removable media connections. This type of approach allows for protecting low impact BES Cyber Systems from the introduction of malicious code into a network that could be used to trigger coordinated cyberattacks in a risk-informed manner.

Nevertheless, the NERC Board, using industry policy input and information gathered from NERC data requests concerning the extent of external connectivity to low impact assets, has recently identified additional areas where the low impact requirements could be modified to better address the risk of a coordinated cyberattack. As noted above, Project 2020-03 will help

address the Commission's concerns with respect to coordinated attacks on geographically dispersed targets by enhancing protections on the external connectivity for low impact BES assets. This includes developing and implementing policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

The industry is also in the process of ensuring compliance with the requirements for Reliability Standard CIP-013-1, which affects medium and high impact assets, and will become effective in October 2020. The purpose of CIP-013-1 is to mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems. Electric companies need time to first observe and understand the implications of these new requirements to medium and high impact assets before determining if further modifications to the standard are needed for high, medium, or low impact assets.

Industry conducts a number of other activities to ensure the reliability and security of the BPS, including participation in exercises such as NERC's bi-annual GridEx drill. GridEx provides a venue for utilities to test and demonstrate how they would respond to and recover from coordinated cyber and physical security attacks and incidents, to strengthen relationships with industry and government partners, and to identify areas for improvement and lessons learned. GridEx VI, planned for Fall 2021, is designed to test incident response plans, involve local and regional industry and government partners as part of the response, engage industry vendors and interdependent cross-sector partners, and improve communication between and amongst all of the stakeholders involved.

The industry regularly participates in several other major exercises that test a broad range of scenarios, and include all levels of government, private industry, and non-governmental organizations. The Department of Energy ("DOE") hosts their ClearPath exercise, focused on energy sector response to natural disasters, annually while their annual Liberty Eclipse exercise examines response cyber capabilities between industry and government partners. The DOE and the Treasury Department also hosted the "Hamilton" series of exercises with industry, testing interdependencies between the electricity and financial sectors. Industry has also participated in a series of cyber exercises focused on blackstart recovery and system restoration hosted by DOE and the Department of Defense. From these exercises, electric companies gain valuable experience and lessons learned in responding to incidents that affect grid reliability and security, and then use those experiences to improve response and recovery. These exercises also help strengthen the relationship between industry and government, allowing better coordination and communication during crises, as well as the development of actionable plans to improve our national security posture.

III. CONCLUSION

The industry faces a broad range of cyber and physical threats and industry uses a number of tools and processes to provide a defense-in-depth approach to security, as well as to prepare for, respond to, and recover from incidents when they occur. The CIP Reliability Standards provide a baseline for strengthening the industry's cybersecurity posture, and through the evaluation of threats, vulnerabilities and resulting risks to determine appropriate tools for addressing the risks, such as modifications to the standards, including Project 2020-03. Due to the dynamic nature of the threat landscape, industry engages in a number of other activities to build upon the foundation provided by the CIP Reliability Standards to protect the grid,

including the application of frameworks such as the NIST Framework, participation in exercises, and engagement in projects and partnerships with the government and other stakeholders. The combination of these complementary approaches allows the industry to efficiently and effectively apply the appropriate tools and allocate resources where needed to provide grid reliability. All of these tools enable electric companies to be well positioned to continue to mitigate threats to the grid from all-hazards, including coordinated cyberattacks. EEI and EPSA appreciate the opportunity to submit comments in response to the NOI. Given the coverage in the existing Reliability Standards and the ongoing projects at NERC to analyze revisions to the CIP Reliability Standards, the Commission should allow NERC and industry to complete their work before pursuing any additional steps to address the NIST Framework issues. Both organizations look forward to continued dialogue with the Commission on these important issues.

Respectfully submitted,

/s/
Andrea Koch
Senior Director, Reliability Policy
akoch@eei.org

Kaitlin Brennan
Senior Manager, Cyber & Infrastructure Security
kbrennan@eei.org

Bob Stroh
Associate General Counsel, Reliability & Security
rstroh@eei.org

Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000

/s/
Nancy Bagot
Senior Vice President
nbagot@epsa.org

Bill Zuretti
Director of Regulatory Affairs & Counsel
bzuretti@epsa.org

Electric Power Supply Association
Washington, D.C. 20005
(202) 628-8200

August 24, 2020